

Cyber Security Threats for Protective Relays



In order to protect the system we need to first understand the threats.

The IEEE PES POWER SYSTEM RELAYING COMMITTEE WORKING GROUP C1 Report on Cyber Security Issues for Protective Relays covers issues concerning the security of electronic communication paths to protective relays. Its goal is to present the reader some background material and discussions that can make them more aware of the concerns associated with electronic communications in the power industry.

The following text is an excerpt from the report that discusses Cyber Security Threats:

In evaluating the security threat to substation equipment, it is apparent that numerous people have physical contact with various devices within the substation. These individuals include employees, contractors, vendors, manufacturers, etc.

Of particular concern is the fact that the typical substation environment can provide a means to compromise the power system with a low probability being detected or apprehended.

This low perceived probability of detection creates opportunities to compromise the operation of the power system which could be attractive for a number of reasons, including:

- Job dissatisfaction
- Economic gain
- Competitor discrediting
- Job security
- Blackmail
- Sport
- Terrorism/Political

The following list provides some examples of possible security threats that may exist in a substation (not to be considered all inclusive).

- A substation automation contractor, with access to the substation, recognizes the station has equipment from a competitor and seeks to discredit that competitor's system by modification of the system configuration.
- An employee concerned about future employment changes all passwords throughout the system so that only they can access the system.
- A third party provider/consumer of power with some authorization to the station arranges to have metering data improperly scaled to support compromised revenue meters.

1 Substation



2 Control center



All components of the infrastructure are subject to cyber security threats.

■ An authorized person is approached by a third party who offers financial reward for the point mapping, address, and password of the automation system.

■ The vendor of the original system has left behind a backdoor which is unknown to the owner and can be used to change the configuration and performance of the system.

It is also important to consider the inadvertent compromise of an IED or automation system by authorized personnel who do not intend to degrade or affect its performance, but through some action on their part, do indeed compromise the device.

Examples include:

■ The use of an outdated or incompatible configuration software version which results in a corruption of the substation device settings.

■ The use/download of an incorrect configuration which results in incorrect settings.

■ Errors in entering settings/configuration data or errors in the engineering development of settings / configuration which compromise the performance of the system.

The intentional and unintentional compromises of the power system are areas of concern for the NERC Cyber Security-Critical Cyber Assets and require addressing in any comprehensive cyber security program.

Threat Sources

In recent years, information security attack technology has become increasingly sophisticated. Attacks have become automated, so that specialized expertise is not necessarily required to perform them. Many attacks install “root kits” on the victim systems which are usually designed to enable the intruder to re-enter the system at will, to prevent the system administrator from discovering the attack, and to destroy any remaining evidence of the attack when the intruder is finished. Threats may be caused by inadvertent actions of authorized persons as well as malicious actions of authorized

and unauthorized persons. Some of the threat sources to consider include:

■ Natural disasters and equipment failure

■ Well-intentioned employees who make inadvertent errors, use poor judgment, or are inadequately trained

■ Employees with criminal intent to profit or to damage others by the misappropriation of utility resources

■ Disgruntled employees or ex-employees who cause damage to satisfy a grudge

■ Hobbyist intruders who gain pleasure from unauthorized access to utility information systems (sport)

■ Criminal activity by both individuals and organizations directed against the utility, its employees, customers, suppliers, or others

■ Terrorists

■ Competing organizations searching for proprietary information of the utility, its suppliers, or customers

■ Unscrupulous participants in the markets for electric power or derivatives

■ Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes

In general, threats are directed towards information held by the utility, but the target of the threat may be an entity other than the utility, such as an employee, customer, or supplier.

For example, reading residential electric use at frequent intervals can provide intruders information on when a residence is unoccupied.

Also, the utility may store data on employees or customers that affects their privacy.

The complete paper can be downloaded from:

<http://www.pes-psrc.org/Reports/Cyber%20Security%20Issues%20for%20Protective%20Relays.pdf> ■

WG Members:

S. Ward (*Chair*),
J. O'Brien (*Co-chair*),
B. Beresh,
G. Benmouyal,
D. Holstein,
J. Tengdin,
K. Fodero,
M. Simon,
M. Carden,
M. Yalla,
T. Tibbals,
V. Skendzic,
S. Mix,
R. Young,
T. Sidhu,
S. Klein,
J. Weiss,
A. Apostolov,
D. Bui,
S. Sciacca,
C. Preuss,
S. Hodder

3 Microwave tower



4 Relays

